IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): J.A. Garay et al.
Docket No.: 8-32
Serial No.: 10/014,763
Filing Date: December 11, 2001
Group: 2132
Examiner: Samson B. Lemma

Title: Methods and Apparatus for Computationally-Efficient Generation of Secure Digital Signatures

---

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313

Sir:

Applicants (hereinafter referred to as "Appellants") hereby appeal the final rejection of claims 1-25 of the above-referenced application.

REAL PARTY IN INTEREST

The present application is assigned to Lucent Technologies Inc. The assignee, Lucent Technologies Inc., is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no known related appeals and interferences.

STATUS OF CLAIMS

Claims 1-25 are pending in the application. Claims 1 and 22-25 are the independent claims.

Claims 2 and 3 stand rejected under 35 U.S.C. §112, second paragraph. Claims 1-7, 9, 10, 17 and 19-25 stand rejected under 35 U.S.C. §102(e). Finally, claims 8, 11-16 and 18 stand rejected under 35 U.S.C. §103(a). All the rejections are traversed.

STATUS OF AMENDMENTS

There have been no amendments filed subsequent to the final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention provides methods and apparatus for the generation of secure digital signatures in an information processing system. The system includes one or more user devices, a signing aid or other intermediary device, and a verifier. See the Specification at, for example, p. 3, lines 5-7.

In accordance with independent claim 1, a method for use in generating digital signatures in an information processing system including a user device, an intermediary device and a verifier, comprises the steps of generating in the user device a first digital signature and sending the first digital signature to the verifier. The verifier, in turn, sends the first digital signature to the intermediary device which checks that the first digital signature is a valid digital signature for the user device. If the first digital signature is valid, the intermediary device generates a second digital signature which is returned to the verifier as a signature generated by the user device.

Independent claim 22 is an apparatus version of claim 1.

Independent claim 23 sets forth an article of manufacture comprising a machine-readable storage medium storing one or more programs that when executed implement the method described by independent claim 1.

Independent claims 24 and 25 set forth methods similar to claim 1. More particularly, in claim 24, the method comprises a step wherein the verifier receives a first digital signature from the user device. In claim 25, the method comprises a step where the intermediary device receives a first digital signature generated by the user device and sent to the intermediary device from the verifier.

The figures help to describe illustrative embodiments of the invention.

For example, FIG. 1 shows an arrangement in which the "information processing system" in claim 1 may correspond to the user device 102, network 104, signing aid 106, verifier 108, certification authority 110 and judge 112. In this arrangement, the signing aid 106 may act as the claimed "intermediary device." FIGS. 3 and 4 go on to show flow diagrams illustrating respective signature setup and signature generation processes in accordance with the claims. For example, step 402 in FIG. 4 may correspond to the steps of "generating in the user device a first digital signature" and "sending the first digital signature to the verifier" in claim 1. Steps 406, 408 and 410 in FIG. 4 may, in turn, correspond to the claimed steps "wherein the verifier sends the first digital signature to the intermediary device, and the intermediary device checks that the first digital signature is a valid digital signature for the user device and if the first digital signature is valid generates a second digital signature which is returned to the verifier as a signature generated by the user device." See the Specification at, for example, p. 4, lines 19-27, and p. 7, line 23 through p. 9, line 3.

Advantageously, the invention allows secure digital signatures to be generated in an efficient manner on a lightweight device such as a mobile telephone, personal digital assistant (PDA) or wearable computer. See the Specification at, for example, p. 3, lines 27-29.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 2 and 3 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite.

2. Claims 1-7, 9, 10, 17 and 19-25 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,711,400 to Aura (hereinafter "Aura").

3. Claims 8, 11-16 and 18 are rejected under 35 U.S.C. §103(a) as being unpatentable over Aura in view of U.S. Patent No. 5,016,274 to Micali et al. (hereinafter "Micali").

ARGUMENT

Appellants incorporate by reference herein the disclosures of all previous responses filed in the present application, namely, responses dated September 6, 2005 and January 10, 2006.

1. Rejection under 35 U.S.C. §112, second paragraph

Claim 2

Dependent claim 2 sets forth:

> The method of claim 1 wherein the first digital signature is generated using a first secret key associated with a first digital signature protocol having a computational efficiency compatible with computational resources of the user device.

In formulating the §112, second paragraph rejection of this claim, the Examiner argues that the limitation "having a computational efficiency compatible with computational resources of the user device" is vague and unclear (Final Office Action, #5). Appellants respectfully disagree. The scope of this limitation would be clear to one skilled in the art in light of the ordinary and customary meanings of the words and their usage in the Specification. Aspects of computational efficiency and computational resources are described in the Specification at, for example, p. 1, lines 12-26 and p. 7, lines 3-8.

Claim 3

Dependent claim 3 sets forth:

> The method of claim 2 wherein the second digital signature is generated using a second secret key associated with second digital signature protocol having a computational efficiency lower than that of the first digital signature protocol.

In formulating the §112, second paragraph rejection of this claim, the Examiner argues that the limitation "having a computational efficiency lower than that of the first digital signature protocol" is vague and unclear (Final Office Action, #6). Appellants respectfully disagree. The

scope of this limitation would be clear to one skilled in the art in light of the ordinary and customary meanings of the words and their usage in the Specification. Aspects of computational efficiency and computational resources are described in the Specification at, for example, p. 1, lines 12-26 and p. 7, lines 3-8.

2. Rejection under 35 U.S.C. §102(e) as being anticipated by Aura

Claims 1, 2 and 19-25

With respect to the §102(e) rejection, Appellants initially note that the Manual of Patent Examining Procedure (MPEP), Eighth Edition, August 2001, §2131, specifies that a given claim is anticipated "only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference," citing Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, MPEP §2131 indicates that the cited reference must show the "identical invention . . . in as complete detail as is contained in the . . . claim," citing Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Claim 1 sets forth:

> A method for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, the method comprising the steps of:
>
> generating in the user device a first digital signature; and
>
> sending the first digital signature to the verifier;
>
> wherein the verifier sends the first digital signature to the intermediary device, and the intermediary device checks that the first digital signature is a valid digital signature for the user device and if the first digital signature is valid generates a second digital signature which is returned to the verifier as a signature generated by the user device.

In formulating the §102(e) rejection of this claim, the Examiner argues that each and every claimed element is anticipated by Aura. More specifically, the Examiner argues that the "authentication centre" in Aura's FIG. 4 (labeled "AUC" in the figure) describes the "user device" in claim 1 (Final Office Action, #10, first bullet point). What is more, the Examiner argues that the

"mobile station" in Aura's FIG. 4 (labeled "MS" in the figure) describes the "intermediary device" in the claim (Final Office Action, #10, fourth and fifth bullet points). Appellants respectfully submit that both assertions are untenable.

In Aura, an authentication centre is connected to a home location register and is a fixed element in a network (Aura, FIG. 1 and col. 1, lines 38-59). The authentication centre performs processing tasks related to authenticating the identity of the network (Aura, col. 5, lines 21-51). In contrast, the user device in claim 1, as the name clearly indicates, is a device that is operated by a user. Embodiments of the user device may comprise, for example, a mobile telephone, PDA, desktop or portable computer, or television set-top box (Specification, p. 5, lines 11-16). As a result, it is clear that Aura's authentication centre does not describe the user device in claim 1.

Aura's mobile station, moreover, comprises mobile equipment and a subscriber identity module (Aura, col. 1, line 66 to col. 2, line 3). A mobile station is operated by a mobile subscriber (i.e., user) (Aura, col. 1, lines 49-59). The intermediary device in claim 1, in contrast, is operative to check that a first signature generated by a user device is valid and to generate a second digital signature which is a returned to the verifier as a signature generated by the user device. Again, it is clear that Aura's mobile station does not describe the intermediary device in claim 1.

Consequently, Aura fails to describe each and every element of claim 1.

Dependent claims 2 and 19-21 are believed to be in condition for allowance for at least the same reasons as their base claim, independent claim 1. Moreover, independent claims 22-25 comprise limitations similar to claim 1 and are believed to be allowable for reasons similar to independent claim 1.

Claim 3

Claim 3 is believed to be in condition for allowance for the same reasons recited above with respect to its base claims, independent claims 1 and dependent claim 2, and, furthermore, is believed to contain separately patentable subject matter with respect to Aura.

Claim 3 sets forth:

> The method of claim 2 wherein the second digital signature is generated using a second secret key associated with second digital signature protocol having a computational efficiency lower than that of the first digital signature protocol.

In formulating the §102(e) rejection of this claim, the Examiner argues that the claimed "second key associated with second digital signature protocol" is anticipated by Aura's secret key "Ki" in FIG. 4 (Final Office Action, #12). Nevertheless, it should be noted that in rejecting claim 2, the Examiner argues that the first key associated with a first digital signature protocol is anticipated by the same secret key "Ki" (Final Office action, #11). Appellants respectfully submit that it is internally inconsistent to argue that Aura's single secret key "Ki" anticipates both the first and second keys set forth in claims 2 and 3.

What is more, unlike claim 3, Aura fails entirely to describe that the second digital signature protocol has "a computational efficiency lower than that of the first digital signature protocol."

Claim 4

Claim 4 is believed to be in condition for allowance for the same reasons recited above with respect to its base claims, independent claim 1 and dependent claims 2 and 3, and, furthermore, is believed to contain separately patentable subject matter with respect to Aura.

Claim 4 sets forth:

> The method of claim 3 wherein an agreement relating to corresponding public keys of the first and second digital signature protocols is signed by both the user device and the intermediary device and the resulting twice-signed agreement is stored by both the user device and the intermediary device.

In formulating the §102(e) rejection of this claim, the Examiner merely argues that the claim is anticipated by Aura's FIG. 4 (Final Office Action, #13). Appellants respectfully disagree. Aura's FIG. 4 does not describe the signing of "an agreement relating to corresponding public keys of the first and second digital signature protocols." Nor does Aura's FIG. 4 describe the storing of the "resulting twice-signed agreement."

Claim 5

Claim 5 is believed to be in condition for allowance for the same reasons recited above with respect to its base claims, independent claim 1 and dependent claims 2 and 3, and, furthermore, is believed to contain separately patentable subject matter with respect to Aura.

Claim 5 sets forth:

> The method of claim 3 wherein the second secret key associated with the second digital signature protocol is supplied from the user device to the intermediary device over a secure private channel.

Like for claim 4, in formulating the §102(e) rejection of claim 5, the Examiner merely argues that claim 5 is anticipated by Aura's FIG. 4 (Final Office Action, #13). Nevertheless, Aura's FIG. 4 fails entirely to describe a "secure private channel." In fact, Aura is careful to point out that Aura's authentication method cannot be defeated by an active eavesdropper listening to the line (Aura, col. 8, lines 3-14).

Claims 6, 7, 9 and 10

Claim 6 is believed to be in condition for allowance for the same reasons recited above with respect to its base claim, independent claim 1, and, furthermore, is believed to contain separately patentable subject matter with respect to Aura.

Claim 6 sets forth:

> The method of claim 1 wherein the first digital signature comprises a signature $s1$ on a message m, the signature $s1$ being generated using a secret key s' of a key pair (s', p') associated with the user device.

In formulating the §102(e) rejection of claim 6, the Examiner argues:

> Furthermore Aura discloses the method wherein **the fist digital signature comprises**

> **a signature s1 on a message m,** [figure 4, ref. 405 and "SRES1"] the **signature s1 being generated using a secret key s'**[figure 4, ref. Num "405" and "Ki"] **associated with the user device.**

Appellants respectfully note, however, that the Examiner fails entirely to point out where Aura generates a signature using a secret key of a key pair, as claimed. Aura, in fact, fails to describe the generation of such a signature.

Like claim 6, claims 7, 9 and 10 each set forth using a secret key of a key pair to generate a signature. Moreover, for each claim, the Examiner's §102(e) rejection is similar to that for claim 6. See Final Office Action, #14-17. Accordingly, these claims are also believed to be in condition for allowance.

Claim 17

Claim 17 is believed to be in condition for allowance for the same reasons recited above with respect to its base claim, independent claim 1, and, furthermore, is believed to contain separately patentable subject matter with respect to Aura.

Claim 17 sets forth:

> The method of claim 1 wherein the intermediary device is configured to wait a predetermined delay period between checking that the first digital signature is a valid signature and generating the second digital signature which is returned to the verifier.

In formulating the §102(e) rejection of this claim, the Examiner argues that all the claim limitations are anticipated by Aura's "408" in FIG. 4 (Final Office Action, #18). Nevertheless, this figure is entirely devoid of any description of a "predetermined delay period." Step 408 in Aura's FIG. 4 is, in fact, a decision step in a flow chart that makes no reference to any kind of delay period.

3. Rejection under 35 U.S.C. §103(a) as being unpatentable over Aura in view of Micali

Claims 8, 11-16 and 18

Dependent claims 8, 11-16 and 18 are believed to be in condition for allowance for at least the same reasons recited above with respect to their base claim, independent claim 1. Moreover, Appellants respectfully submit that the §103(a) rejection of these claims is deficient.

A *prima facie* case of obviousness can only be established if there is "some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings." MPEP §2143. Any such showing of obviousness "must be based on objective evidence of record" rather than "subjective belief and unknown authority." In re Sang-Su Lee, 277 F.3d 1338, 1343-44, 61 USPQ2d 1430 (Fed. Cir. 2002).

With respect to the motivation to combine aspects of Aura with Micali, the Examiner states at #22 in the Final Office Action:

> It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of verification digitat [*sic*] signature using the public key as per teaching of Micali in to the method verification as taught by **Aura**, in order to enhances [*sic*] the security and efficiency of known signature schemes. [See Micali Column 1, lines 7-9].

Clearly, in contravention to the requirements for a valid §103(a) rejection, the above-quoted argument lacks any basis in objective evidence of record that would motivate one skilled in the art to combine the references as suggested. Instead, the Examiner has apparently used improper hindsight by using the Appellant's teachings as a blueprint to hunt through the prior art for the claimed elements and combine them as claimed. The result is an argument to combine references that finds its true motivation in advantageous aspects of the present invention. The Federal Circuit has repeatedly held that such an approach is "an illogical and inappropriate process by which to determine patentability." Sensonic, Inc. v. Aerosonic Corp., 81 F.3d 1566, 1570, 38 USPQ2d 1551, 1554 (Fed. Cir. 1996).

In view of the above, Appellants respectfully request the withdrawal of the §§112, 102(e) and 103(a) rejections.

Respectfully submitted,

Date: April 24, 2006

Michael L. Wise
Attorney for Appellant(s)
Reg. No. 55,734
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2722

CLAIMS APPENDIX

1. A method for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, the method comprising the steps of:

generating in the user device a first digital signature; and

sending the first digital signature to the verifier;

wherein the verifier sends the first digital signature to the intermediary device, and the intermediary device checks that the first digital signature is a valid digital signature for the user device and if the first digital signature is valid generates a second digital signature which is returned to the verifier as a signature generated by the user device.

2. The method of claim 1 wherein the first digital signature is generated using a first secret key associated with a first digital signature protocol having a computational efficiency compatible with computational resources of the user device.

3. The method of claim 2 wherein the second digital signature is generated using a second secret key associated with second digital signature protocol having a computational efficiency lower than that of the first digital signature protocol.

4. The method of claim 3 wherein an agreement relating to corresponding public keys of the first and second digital signature protocols is signed by both the user device and the intermediary device and the resulting twice-signed agreement is stored by both the user device and the intermediary device.

5. The method of claim 3 wherein the second secret key associated with the second digital signature protocol is supplied from the user device to the intermediary device over a secure private channel.

6. The method of claim 1 wherein the first digital signature comprises a signature $s1$ on a message m, the signature $s1$ being generated using a secret key s' of a key pair (s', p') associated with the user device.

7. The method of claim 1 wherein the first digital signature comprises a signature $s1$ on $h(m)$, where m is a message and h is a hash function, the signature $s1$ being generated using a secret key s' of a key pair (s', p') associated with the user device.

8. The method of claim 3 wherein the verifier upon receipt of the first digital signature checks that the first digital signature is a valid digital signature using a first public key corresponding to the first secret key.

9. The method of claim 1 wherein the second digital signature comprises a signature $s2$ on a message m, the signature $s2$ being generated using a secret key s of a key pair (s, p) associated with the user device.

10. The method of claim 1 wherein the second digital signature comprises a signature $s2$ on $h(m)$, where m is a message and h is a hash function, the signature $s2$ being generated using a secret key s of a key pair (s, p) associated with the user device.

11. The method of claim 2 wherein the verifier upon receipt of the second digital signature checks that the second digital signature is a valid digital signature using a second public key corresponding to the second secret key.

12. The method of claim 1 wherein the user device is switchable between a normal operating mode and a secure operating mode.

13. The method of claim 1 wherein the first digital signature is generated only after user verification of the message to be signed.

14. The method of claim 1 wherein at least one of first and second secret keys used to generate the respective first and second and second digital signatures are stored in an at least partially encrypted form on the user device and the intermediary device, respectively.

15. The method of claim 1 wherein at least one of first and second secret keys used to generate the respective first and second and second digital signatures is configured such that a first portion thereof is stored in the user device and a second portion thereof is stored in a storage element removable from the user device.

16. The method of claim 1 wherein if a user associated with the user device can contact the intermediary device and upon providing an access code thereto direct the intermediary device not to generate the second digital signature.

17. The method of claim 1 wherein the intermediary device is configured to wait a predetermined delay period between checking that the first digital signature is a valid signature and generating the second digital signature which is returned to the verifier.

18. The method of claim 1 wherein the user device precomputes a plurality of coupons, a given one of the coupons being utilizable to generate the first digital signature.

19. The method of claim 1 wherein the user device comprises a mobile telephone.

20. The method of claim 1 wherein the user device comprises a personal digital assistant (PDA).

21. The method of claim 1 wherein the user device comprises a wearable computer.

22. An apparatus for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, the apparatus comprising:

a memory; and

a processor coupled to the memory, the processor being operative to generate in the user device a first digital signature, and to send the first digital signature to the verifier;

wherein the verifier sends the first digital signature to the intermediary device, and the intermediary device checks that the first digital signature is a valid digital signature for the user device and if the first digital signature is valid generates a second digital signature which is returned to the verifier as a signature generated by the user device.

23. An article of manufacture comprising a machine-readable storage medium for storing one or more programs for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, wherein the one or more programs when executed implement the steps of:

generating in the user device a first digital signature; and

sending the first digital signature to the verifier;

wherein the verifier sends the first digital signature to the intermediary device, and the intermediary device checks that the first digital signature is a valid digital signature for the user device and if the first digital signature is valid generates a second digital signature which is returned to the verifier as a signature generated by the user device.

24. A method for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, the method comprising the steps of:

receiving in the verifier from the user device a first digital signature; and

sending the first digital signature from the verifier to the intermediary device;

wherein the intermediary device checks that the first digital signature is a valid digital signature for the user device and if the first digital signature is valid generates a second digital signature which is returned to the verifier as a signature generated by the user device.

25. A method for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, the method comprising the steps of:

receiving in the intermediary device a first digital signature generated in the user device and sent to the intermediary device from the verifier;

checking in the intermediary device that the first digital signature is a valid digital signature for the user device; and

if the first digital signature is valid generating a second digital signature which is returned to the verifier as a signature generated by the user device.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None